

#Configurazione# Configurazione di un Destination NAT (DNAT) su Sangfor NGAF V8.0.85

***Prodotto:** NGAF

***Versione:** 8.0.85

*1. Introduzione

1.1 Scenario

Sangfor DNAT (Destination Network Address Translation) è una funzionalità presente sui prodotti Sangfor IAM (Internet Access Management) e NGFW (Next-Generation Firewall).

DNAT (Destination Network Address Translation) è un metodo di routing utilizzato per permettere ad un firewall di tradurre un ip di destinazione in un altro ip di destinazione.

Di seguito vengono riportati dei punti chiave riguardo Sangfor DNAT:

- Viene usato per reindirizzare il traffico in arrivo su un host od un server specifico all'interno della rete locale.
- Viene spesso usato per dare accesso dall'esterno a dispositivi che sono nella rete locale.
- Può essere configurato nelle interfacce web dei prodotti Sangfor IAM ed NGFW.
- La configurazione permette di impostare l'ip originale con relativa porta di destinazione e l'ip e porta di destinazione finale di traduzione.
- Questo aspetto è utile per scenari in cui si vuole esporre un servizio od un'applicazione locale su internet.

Di seguito in questa guida, vedremo i passaggi da seguire per pubblicare una risorsa locale.

1.2 Requisiti

1. Firewall Sangfor NGAF aggiornato all'ultima versione

2. Indirizzo ip e porta usati dalla risorsa locale che si vuole dare accesso dall'esterno

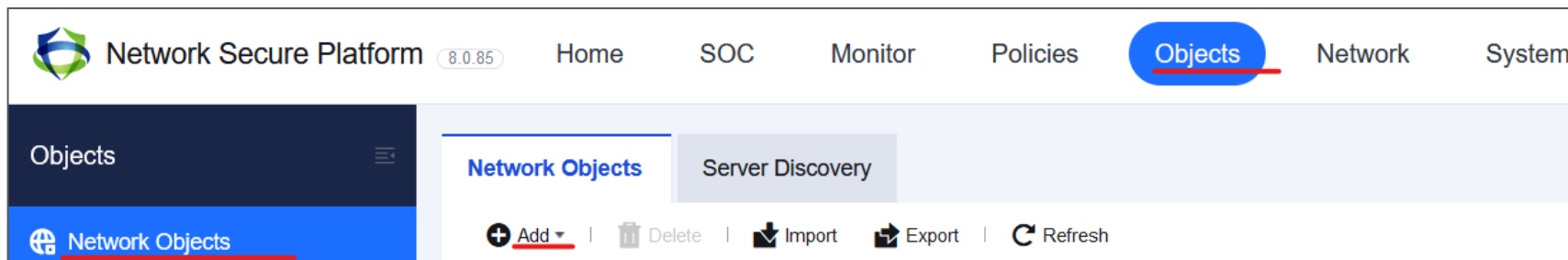
*2. Configurazione

In questa guida, abbiamo la rete locale 10.0.0.0/24 e si vuole pubblicare un server web locale (apache2) raggiungibile internamente con l'ip 10.0.0.5 sulla porta 20443

2.1 Configurazione DNAT NGAF DNAT

Passo 1. Controllare attentamente le zone definite nel firewall e configurare i relativi oggetti di rete su NGAF.

Per far ciò, occorre recarsi nella seguente sezione di NGAF:



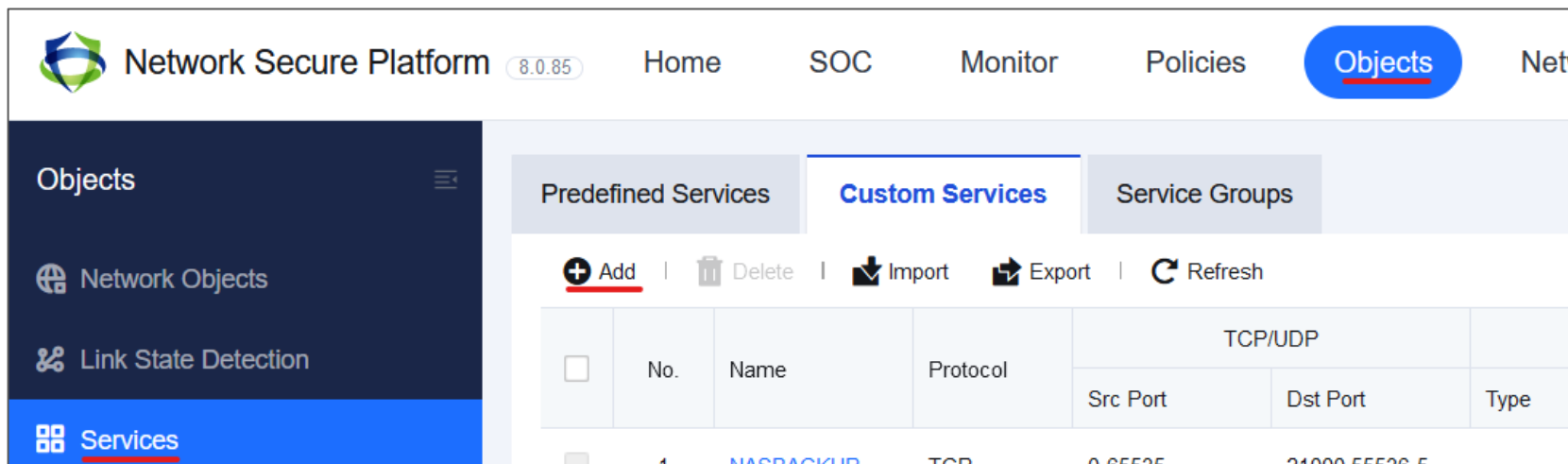
In questo esempio abbiamo:

Zona Sorgente: L3_WAN (la nostra wan)

IP Pubblico: UTGNET (il nostro provider)

L'ip del webserver locale: PHPIPAM (il nostro webserver che si vuole pubblicare)

Passo 2. Creare un oggetto servizio custom dato che dobbiamo usare la porta 20443 TCP. Per far ciò, occorre recarsi nella seguente sezione di NGAF:



The screenshot displays the NGAF web interface. The top navigation bar includes the 'Network Secure Platform' logo, version '8.0.85', and tabs for 'Home', 'SOC', 'Monitor', 'Policies', and 'Objects' (which is highlighted with a blue circle). A left sidebar contains 'Objects', 'Network Objects', 'Link State Detection', and 'Services' (highlighted with a blue bar). The main content area has three tabs: 'Predefined Services', 'Custom Services' (selected), and 'Service Groups'. Below these tabs are action buttons: '+ Add' (underlined in red), 'Delete', 'Import', 'Export', and 'Refresh'. A table lists services with columns: No., Name, Protocol, TCP/UDP (subdivided into Src Port and Dst Port), and Type. The first row shows a service with No. 1, Name NASBACKUP, Protocol TCP, Src Port 0.65525, Dst Port 21000.55528.5, and Type 5.

No.	Name	Protocol	TCP/UDP		Type
			Src Port	Dst Port	
1	NASBACKUP	TCP	0.65525	21000.55528.5	5

Nel nostro esempio ho creato un oggetto servizio custom chiamato IPAM_20443

Edit Custom Service

X

Name:

IPAM_20443

Description:

Optional

Protocols

+


Add

🗑

Delete

<input type="checkbox"/>	Protocol	TCP/UDP		ICMP/ICMPv6		Operation	...
		Src Port	Dst Port	Type	Code		
<input type="checkbox"/>	TCP	0-65535	20443	-	-	<a>Edit <a>Delete	

Passo 3. Creare ora un oggetto DNAT nella seguente sezione:


Network Secure Platform
(8.0.85)
Home
SOC
Monitor
Policies
Objects
Network
System
Menu

Policies

Access Control

NAT

IPv4 NAT

IPv6 NAT

NAT64

DNS-Mapping

+ Add | 🗑️ Delete | ✓ Enable | ⚙️ Disable | ↕ Move To | ... More | ↻ Refresh
All

	No.	Name	Type	Original Data Packet			
<input checked="" type="checkbox"/>				Src Zone	Src Address	Dst Zone/Interface	Dst Address
				Services			

Selezionare Destination NAT usando gli oggetti creati nei passi precedenti.

Di seguito potete vedere che non uso una porta interna diversa dalla porta esterna.

Di conseguenza, lascio bianco il campo Translate Port to

Edit IPv4 NAT

Type: ☐ Source NAT ☒ Destination NAT ☐ Bidirectional NAT

Basics

Name: DNAT_IPAM_20443

Status: ☒ Enabled ☐ Disabled

Description: Optional

Schedule: all-week

Original Data Packet

Src Zone: L3_WAN

Src Address: All

Destination: ☐ IP Address ☒ Network Objects

UTGNET

Services: IPAM_20443

Translated Data Packet

Translate Src IP To: Untranslated

Translate Dst IP To: Network Object

Network Object: PHPIPAM

Translate Port To: Optional, such as internal server port

To make NAT policy work, please configure local ACL or application control policy.

Allow: ☐ Add ACL policy automatically ☒ Add ACL policy manually [Add](#)

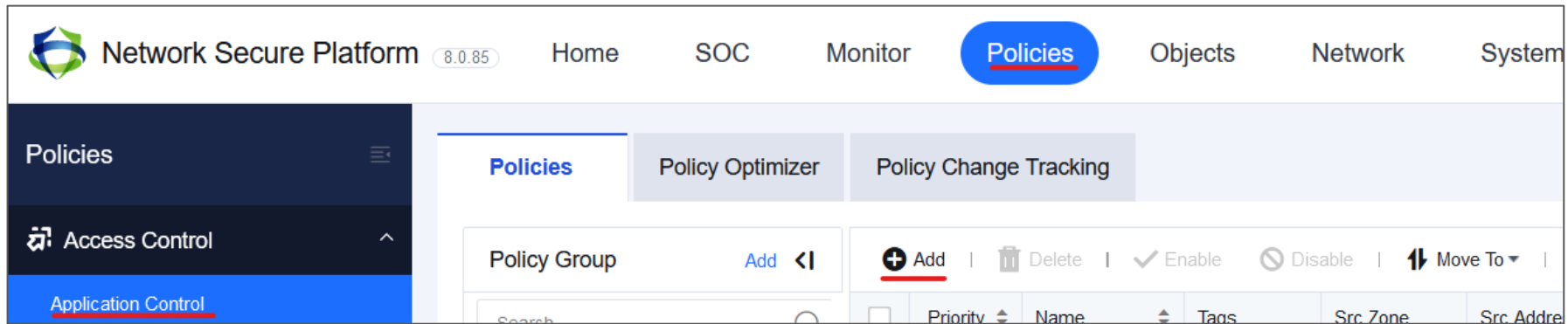
Logging: ☒ Log application control logs

Save Cancel

2.2 Configurazione policy NGAF

Passo 1. Nell'ultimo passaggio, se si sceglie di aggiungere automaticamente la policy ACL (Add ACL Policy automatically), si verrà reindirizzati nella sezione relativa alle policy dell'interfaccia web di NGAF.

Personalmente suggerisco di creare manualmente la policy su NGAF come segue:



Nel nostro esempio, ho creato una regola di controllo applicativa (application control rule) come segue:

Edit Application Control Policy



Basics

Name:

Status: ☒ Enabled ☐ Disabled

Description:

Policy Group:

Tags:

Source

Src Zone:

Src Address: ☒ Network Objects ☐ MAC Address

User/Group:

Destination

Dst Zone:

Dst Address: ☒ Network Objects ☐ MAC Address

Services:

Applications:

Others

Action: ☒ Allow ☐ Deny

Save

Cancel

***3. Attenzione**

Quando si crea un oggetto service custom, è importante specificare 0-65535 come intervallo di porte sorgente, dato che non si può sapere la porta che viene usata dall'esterno per accedere alla risorsa pubblicata.